PUBLIC VERSION

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Dealer Management Systems Antitrust Litigation, MDL 2817	No. 1:18-CV-864
This filing relates to: *Authenticom, Inc. v. CDK Global, LLC et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr.

DEFENDANT CDK GLOBAL, LLC'S OPPOSITION
TO PLAINTIFF'S MOTION TO DISMISS COUNTERCLAIMS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

PUBLIC VERSION

TABLE OF AUTHORITIES
(continued)

Page(s)

PUBLIC VERSION

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes, Rules and Regulations

Other Authorities

INTRODUCTION

Authenticom has built its business on unauthorized access to CDK's dealer management system ("DMS"). Indeed, it is wholly dependent on such access to extract data and monetize it. It thus is unsurprising that Authenticom has continued to use deceptive means to access the DMS despite CDK's efforts to prevent such access, including by bypassing security measures and giving knowingly false responses to security prompts. Those acts of unauthorized access—and outright fraud—give rise to a host of legal claims, all of which are pled in detail in CDK's counterclaims.

Authenticom's principal (and, in many instances, only) response to these claims is to argue that CDK's dealer contracts permit dealers to give Authenticom access to the DMS. But that argument flies in the teeth of the text of the relevant contracts and, at a minimum, cannot be resolved in Authenticom's favor on a motion to dismiss. Authenticom's other quibbles with the sufficiency of CDK's counterclaims are equally misplaced. Accordingly, the Court should deny the motion to dismiss in its entirety.

FACTUAL BACKGROUND

A. CDK's DMS

CDK is one of the country's leading firms offering state-of-the-art enterprise software, known as dealer management systems ("DMS") and related services, to Auto, Truck, Motorcycle, Marine, Recreational Vehicle, and Heavy Equipment dealerships. Counterclaim Compl. (Dkt. 230) ¶ 1. CDK's DMS provides dealers with proprietary software tools and resources necessary to manage core aspects of their business. *Id.* CDK has invested hundreds of millions of dollars to develop the hardware and software components of the DMS. CDK's DMS also includes, and is largely comprised of, valuable pieces of intellectual property, including patented technologies and proprietary software elements and programs created by CDK, each of which are accessed each time a user logs into and uses the DMS. *Id.* ¶ 19.

In addition to its core functionalities, the CDK DMS manages voluminous amounts of financial and accounting information and highly sensitive data, including financial statements, accounting data, payroll information, sales figures, inventory, parts data, warranty information, appointment records, service and repair records, vehicle information, customer personal identifiable information, intellectual property, and other third-party data. CDK encrypts sensitive data in the DMS and appropriately expunges data regularly. Counterclaim Compl. ¶ 22.

The data on CDK's DMS is comprised of proprietary data of many different entities. Some data is proprietary to auto manufacturers, such as prices and part numbers for replacement parts, labor rates, and rebate, incentive and warranty information. Counterclaim Compl. ¶ 23. Other data in CDK's DMS is proprietary to third-party service providers, such as credit reporting bureaus like Equifax, Experian, and TransUnion. *Id.* Still other data in the DMS is CDK's own proprietary data, including forms, accounting rules, tax tables, and proprietary tools and data compilations. *Id.* While access to third-party proprietary information in the DMS is permitted for licensed DMS customers, CDK is prohibited from sharing much of this information with unlicensed third parties. *Id.* And CDK generally does not share its own proprietary information in the DMS with any third parties in the absence of a valid license. *Id.*

Given the sensitivity of the data that resides on the DMS, and the demands of the technical infrastructure that allows it to operate, it is essential for CDK to maintain control over who accesses the DMS and to prevent access by persons who do not have CDK's permission to use it. Accordingly, CDK's DMS service contract with dealers (the Master Services Agreement, or "MSA") expressly prohibits dealers from granting any unauthorized third-party access to the DMS, including by creating login credentials for third parties. Counterclaim Compl. ¶ 71. CDK has employed such a provision in its MSA since 1994. *Id.* ¶ 73.

B. Authenticom's data extraction practices

Authenticom, though it refers to itself as a "dealer data integration provider," is essentially a data extractor. Counterclaim Compl. ¶ 40. Its business model involves accessing CDK's DMS (and other DMSs) using login credentials provided by dealers, extracting and exporting the data from those DMSs, often copying the data into its own system, and then selling the data to third parties—principally vendors providing software applications to dealers (such as sales applications or service scheduling applications). *Id.* ¶ 42. This practice sweeps up a tremendous amount of sensitive data, given that CDK's DMS stores not only data generated by dealers but also proprietary data belonging to third parties such as auto manufacturers and credit reporting bureaus. *Id.* ¶¶ 22-23.

Authenticom has recently begun asserting (in this litigation) that its access to CDK's DMS is permitted, notwithstanding the MSA's prohibition on unauthorized third-party access, because the MSA allows access by dealers' "agents." Counterclaim Compl. ¶ 75. But Authenticom specifically disavows having any agency relationship with the dealers it services, proclaiming itself instead to be an independent contractor. *Id.* And ironically, like defendants' agreements with dealers, Authenticom's service agreements with dealers forbid dealers from granting login credentials to any unauthorized third parties. *Authenticom* Dkt. 65-3, § 6.7 (noting that a password will be issued to "each User authorized to use Dealership's account").

C. CDK's decision to enforce the access restrictions in its DMS contracts

At one time, CDK did not actively enforce its contractual right to block hostile integrators like Authenticom. Counterclaim Compl. ¶ 76. But events in recent years—particularly in 2013 and 2014—changed CDK's thinking about the risks of third-party access to the DMS. During that time frame, a number of high-profile data breaches occurred, causing millions of dollars in damage and compromising sensitive information for millions of the affected companies' customers. *Id.* ¶ 77. And in late 2014, CDK was spun off from its parent, ADP, and became a stand-alone public company—which focused its leadership's attention on the risks the company ran by tacitly permitting dealers to

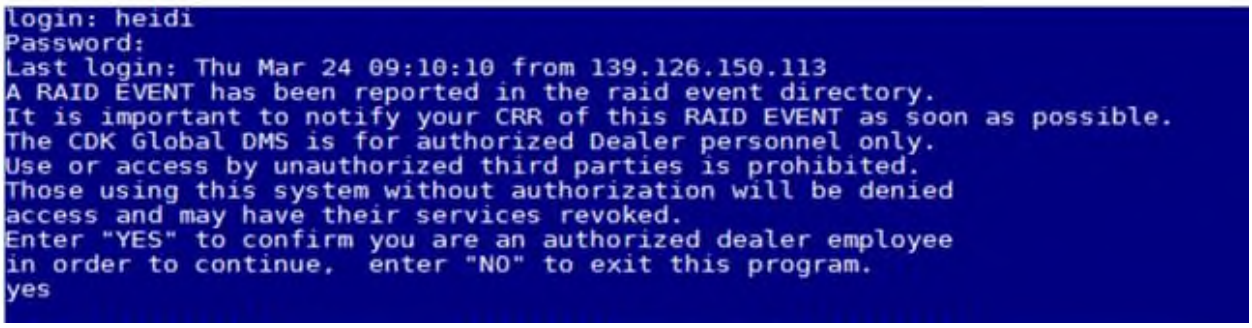
give DMS access to whomever they wished. *Id.* ¶ 79. CDK also became concerned that its failure to enforce its access policies was permitting hostile integrators like Authenticom to free-ride on CDK's significant investments in its DMS and the associated intellectual property—reaping profits for themselves without paying CDK anything in return. *Id.* And CDK was becoming increasingly aware that hostile integration was infecting the DMS with hostile computer code and creating a host of data corruption issues. *Id.* ¶¶ 57, 81.

In response to these concerns, CDK announced a new multipart strategy called "SecurityFirst" in June 2015. Counterclaim Compl. ¶ 81. One aspect of the program was an initiative to remove third-party code installed on the DMS and eliminate unauthorized third-party access, including through the use of dealer-issued login credentials. *Id.* As part of SecurityFirst, vendors and other third parties may obtain access to CDK's DMS only through a revamped version of CDK's Third Party Access or "3PA" managed interface, which allows third parties to extract data from and write data to CDK's DMS in a controlled manner, using predefined integration points tailored to the specific needs of each third party. *Id.* ¶¶ 27-28.

D. Authenticom's bad acts

Even after CDK announced the revamped 3PA program and began blocking unauthorized hostile access to the DMS, Authenticom continued to encourage dealers to share login credentials, seeking continued access to the DMS in violation of the dealers' service agreements with CDK. Given the threats this unauthorized access posed to the security and stability of the DMS, CDK took steps to block unauthorized access and restrict DMS use to authorized dealer employees.

Authenticom has been purposeful and reckless in its attempts to circumvent these measures. At one point, for example, CDK implemented a security measure that prompted a user logging in to the system to confirm that the user was an authorized dealer employee:



CDK's security records show that Authenticom-linked credentials began responding "yes" automatically to this prompt soon after CDK began using it. Counterclaim Compl. ¶ 85. In other words, Authenticom modified the hostile data extraction scripts it used to access the DMS to falsely certify that it was a dealer employee. *Id.*

Authenticom also used software workarounds to automatically reinstate dealer-supplied login credentials that CDK had deactivated in accordance with its dealer agreements. In particular, Authenticom created and implemented a software tool that would automatically re-enable any disabled user IDs "every hour." Counterclaim Compl. ¶ 63. [redacted] To this day, Authenticom continues to extract data from CDK's DMS, in violation of the dealers' DMS service agreements.

ARGUMENT

The only question currently before this Court is whether CDK's counterclaims allege "sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *AnchorBank, FSB v. Hofer*, 649 F.3d 610, 614 (7th Cir. 2011) (internal quotation marks omitted). In making that determination, the Court must evaluate the counterclaim complaint "in the light most favorable to [CDK], taking as true all well-pleaded factual allegations and making all possible inferences from the allegations in [CDK's] favor." *Id.* The bar set by Rule 12(b)(6) "is not high," and CDK's well-pled allegations easily overcome it. *Id.* (internal quotation marks omitted).

I. CDK HAS PLAUSIBLY ALLEGED THAT AUTHENTICOM'S DMS ACCESS IS UNAUTHORIZED.

Authenticom's motion to dismiss repeatedly raises one overarching issue: *i.e.*, whether Authenticom was authorized to access CDK's DMS pursuant to an MSA provision prohibiting dealers from making the DMS available "to any person other than employees and agents of [the dealer] with a need-to-know." *See* Counterclaim Compl. ¶ 75. Authenticom argues that it is an "agent" of the dealers with whom it contracts, and its principal (and often only) defense to CDK's counterclaims is that dealers authorized it to access the DMS. But CDK's complaint easily states a claim that such is not the case.

The complaint provides ample detail on this point. It alleges that multiple sections of the MSA prohibit access by third parties and third-party software. Counterclaim Compl. ¶¶ 71-72 (citing MSA §§ 4(B), 4(D)). It alleges that Authenticom is not an authorized dealer "agent" and has known as much for many years. *Id.* ¶ 74. It alleges that Authenticom in fact *disavows* that it is an agent of dealers. *Id.* ¶ 75. And it alleges that, in any event, whether Authenticom is an agent of dealers is moot because the MSA independently prohibits DMS access by "third party software." *Id.*

Authenticom argues that this Court can nonetheless decide at the pleading stage that Authenticom fits into the MSA's former provision permitting access by "employees and agents." Mot. 5.[1] But to decide that question at the pleading stage, the Court would need to find that the MSA unambiguously permitted dealers to give access to third parties like Authenticom. *See, e.g.*, *McWane, Inc. v. Crow Chicago Indus., Inc.*, 224 F.3d 582, 584 (7th Cir. 2000) (explaining that "*[i]f* the district court determines that the contract is unambiguous, it may determine its meaning as a matter of law") (emphasis added). "[I]f the court finds that the contract is ambiguous, the contract's

[1] In support of this argument, Authenticom refers at times to the transcript of the preliminary injunction hearing and to Judge Peterson's opinion on the injunction. *E.g.*, Mot. 5, 7 n.4. Those references should be disregarded, because the Court's inquiry here is limited to the counterclaim complaint and documents incorporated by reference. And in any event, it is well understood that, to the extent based on Judge Peterson's injunction opinion, "the findings of fact and conclusions of law made by a court granting a preliminary injunction are not binding" on a court at later stages of the litigation. *Univ. of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981).

meaning becomes a fact question for the trier-of-fact." *Metalex Corp. v. Uniden Corp. of Am.*, 863 F.2d 1331, 1333 (7th Cir. 1988). And there is simply no basis upon which the Court could conclude at this stage that the MSA not only permitted dealers to give access to Authenticom, but did so unambiguously.

To begin with, although Authenticom attempts to show that it is dealers' "agent" under the law of agency, it is exceedingly unlikely that the term "agent" in the MSA means any third party with whom Authenticom forms a common-law agency relationship. It strains credulity that CDK, despite placing numerous provisions in the MSA aimed at restricting unauthorized access to the DMS, would nonetheless permit dealers unilaterally to designate *any* person or entity they chose as their "agent" and thereby grant that "agent" unfettered access to CDK's DMS, free of charge.

Authenticom's reliance on *Hernandez ex rel. Gonzalez v. Tapia*, decided by another court in this district, is therefore misplaced. In *Hernandez*, the court held that the phrase "agents and employees" was unambiguous as used in the release agreement at issue in that case; it did not hold that those words are always unambiguous in every contract. 2010 WL 5232942, at *7 (N.D. Ill. Dec. 15, 2010). Here, in the context of a contract restricting dealers' ability to give DMS access to third parties or third-party software, it is far from clear that dealers are free to designate any third party they please as their "agent" (indeed, CDK submits the exact opposite is true). The ambiguity over the scope of the term "agency" alone forecloses Authenticom's effort to have CDK's counterclaims decided at the pleading stage.[2]

Even if it were undisputed that the MSA means "agency" in the common-law sense, Authenticom has not demonstrated that it is dealers' common-law agent, and it cannot do so on the pleadings. Under the law of Wisconsin (which governs Authenticom's DealerVault contracts (*see*

[2] In its reply in support of its motion to dismiss Authenticom's claims, CDK discussed the elements of common-law agency. *Authenticom* Dkt. 219 at 16. But CDK did not thereby concede that the term "agent" in the MSA tracks the definition of common-law agency. CDK described the law merely to illustrate the sort of allegations that Authenticom, at a minimum, would have had to make to raise a plausible inference that it is covered by the "agents" provision.

Authenticom Dkt. 65-3 § 10.6),[3] agency "requires 'an agreement of two parties, embodying three factual elements: (1) the manifestation of the principal that the agent is to act for him; (2) the agent's acceptance of the undertaking; and (3) the understanding of the parties that the principal is to control the undertaking.'" *Scheurer v. Fromm Family Foods LLC*, 863 F.3d 748, 755 n.4 (7th Cir. 2017) (quoting *Norton v. Am. Home Mortg. Servicing, Inc.*, 2011 WL 5828122, at *2 (E.D. Wis. Nov. 18, 2011)). "Mere authority to act for another does not, without more, establish agency since independent contractors, as well as agents, both act on behalf of a principal." *Norton*, 2011 WL 5828122, at *2 (citing *Envirologix Corp. v. City of Waukesha*, 531 N.W.2d 357, 365 (Wis. Ct. App. 1995)). "The critical distinction between an independent contractor and an agent is the degree of control exercised by the principal." *Id.*

Authenticom has not shown, and CDK's counterclaims certainly do not support any conclusion, that dealers exercise sufficient control over Authenticom's "undertaking" to make Authenticom their agent. If anything, Authenticom would be the agent of *vendors*, who pay it to extract data—not dealers, who merely purport to give it DMS access to facilitate that extraction. The most that Authenticom can point to is that dealers provide it with login credentials; [redacted] and that dealers purportedly tell Authenticom what data it may pull. Mot. 7 & n.4. Even if all the foregoing were true, none of it demonstrates *control*: these allegations would show, *at most*, that Authenticom does the work dealers permit it to do, when dealers permit it to do the work—just as an independent contractor would.

Moreover, Authenticom's own contracts require dealers to agree that Authenticom is an

[3] The analysis would be largely the same under Illinois or New Jersey law, which are chosen as the applicable law in various versions of the MSA. Both states' laws likewise require a showing that the principal exercises control over the agent's work. *See, e.g.*, *Knapp v. Hill*, 657 N.E.2d 1068, 1071 (Ill. App. 1995) ("The test of agency is whether the purported principal has the right to control the manner and method in which the work is carried out by the agent and whether the agent is capable of subjecting the principal to personal liability."); *Sears Mortg. Corp. v. Rose*, 634 A.2d 74, 79 (N.J. 1993) ("An agency relationship is created when one party consents to have another act on its behalf, with the principal controlling and directing the acts of the agent."). And as explained *infra*, Authenticom has not alleged facts sufficient to show control here.

"independent contractor[]." *Authenticom* Dkt. 65-3 § 10.4. Authenticom suggests that this express contract language should be ignored, but the cases it cites offer no support for that approach. *Automation by Design, Inc. v. Raybestos Products Co.*, 463 F.3d 749, 757 (7th Cir. 2006), involved an agency question decided on summary judgment—not on a motion to dismiss. And in *Priority International Animal Concepts, Inc. v. Bryk*, 2012 WL 1995113, at *5 (E.D. Wis. June 1, 2012), the plaintiff's complaint alleged in certain places that the defendant was its agent—contradicting its claim elsewhere that he was not—and the parties' employment contract further stated that the defendant *was* the plaintiff's agent in certain situations. Those facts are a far cry from the facts here, where Authenticom previously sought to disavow any agency relationship with dealers, only to change its tune for purposes of this litigation.

Authenticom also argues that its disavowal of an "employment agency" relationship does not apply here because that disclaimer means only that "Authenticom is not the dealers' *employee*." Mot. 9. But if the parties had intended to accomplish only that result, they would have said simply "employment," not "employment agency." Contract language "should be construed to give meaning to every word" (*Md. Arms Ltd. P'ship v. Connell*, 786 N.W.2d 15, 25 (Wis. 2010))—and the reading that gives meaning to the word "agency" is that the parties merely omitted an intended comma between "employment" and "agency": "The Parties expressly agree that they are independent contractors and do not intend for these Terms and Conditions to be interpreted as an employment[,] agency, joint venture, or partnership relationship." *Authenticom* Dkt. 65-3, § 10.4. Indeed, the alternative reading—which would have Authenticom disclaiming that it is an "employment agency"—is absurd.

Authenticom also argues that "[i]ndependent contractors can be—and frequently are—agents." Mot. 9. But even if independent contractors are *sometimes* agents, Authenticom and its dealer clients "expressly" agree not to create an "agency" relationship. *Id.*

In short, the text of the MSA and Authenticom's own dealer contracts conclusively refute Authenticom's claim that it is dealers' "agent" within the meaning of the MSA. And even if there were doubt on the point, the issue cannot be resolved in Authenticom's *favor* based on the text of these contracts alone—particularly in light of the freestanding contractual provision prohibiting DMS access by third party software. Counterclaim Compl. ¶ 75. The Court should therefore reject Authenticom's argument as a basis for dismissal, as this and other courts have done in similar circumstances. *See, e.g.*, *Restoration Specialists, LLC v. Hartford Fire Ins. Co.*, 2009 WL 3147481, at *3 (N.D. Ill. Sept. 29, 2009) (Dow, J.) ("[T]he question of agency typically presents an issue of fact that seldom can be resolved at the summary judgment stage, much less on a motion to dismiss."); *Semitekol v. Monaco Coach Corp.*, 582 F. Supp. 2d 1009, 1024 (N.D. Ill. 2008) ("[W]hether an agency relationship has been established between the parties is one of fact [sic] which is not properly resolved on a motion to dismiss.").

II. AUTHENTICOM'S OBJECTIONS TO SPECIFIC COUNTERCLAIMS ARE MERITLESS.

The inability to resolve Authenticom's agency defense in its favor on the pleadings disposes of most of Authenticom's motion to dismiss CDK's counterclaims. *See* Mot. 11, 17, 23 (relying on Authenticom's purported authorization to access the DMS as the only basis for dismissing Counts 1, 4, 6, 7, 8, and 9).[4] Authenticom's remaining arguments are equally meritless.

A. CDK has stated a claim under the CFAA and parallel Wisconsin and California statutes (Counts 1, 4, and 6)

To begin with, the failure of Authenticom's "authorization" argument is fatal to its motion to dismiss CDK's claims under the Computer Fraud and Abuse Act ("CFAA"), the Wisconsin Computer Crimes Act, and the California Comprehensive Computer Data Access and Fraud Act,

[4] Authenticom also argues that Count 7, CDK's counterclaim under the California Unfair Competition Law ("UCL"), must be dismissed to the extent it relies on the UCL's "unlawful" conduct prong because there is no surviving claim of unlawful conduct on which that claim can be based. Mot. 23. But because Authenticom's motion to dismiss Counts 1. 4. 6. 8, and CDK's claim under the "unfair" practices prong of the UCL based on the authorization issue fails, its motion to dismiss CDK's allegations under the "unlawful" prong fails as well.

given that Authenticom's only argument for dismissing these claims is that the MSA permitted dealers to grant it access to the DMS. Authenticom has conceded as much by *not* moving to dismiss parallel counterclaims brought by Reynolds, whose dealer contracts do not have the "agent" language that Authenticom has hung its hat on.

But even if Authenticom were right about the meaning of the MSA (and it is not), these claims still could not be dismissed. Authenticom's motion presumes that, if the MSA permitted dealers to give Authenticom access, its DMS access could not have been "unauthorized" for CFAA purposes—but that is incorrect. As Judge Easterbrook pointed out at the Seventh Circuit oral argument, the "authorization" required for lawful access under the CFAA must come from the owner of the computer system, not from anyone who happens to use the system. Dkt. 256-7 at 51:7-11 ([Judge Easterbrook]: "This [*i.e.*, the CFAA] doesn't say, permission by anyone. If I have an account with AOL, . . . to get access to AOL's system, you need AOL's permission, not my permission."). And by no later than June 2015, CDK had clearly put Authenticom on notice that, as the owner of the DMS, CDK was refusing to authorize Authenticom's access to the DMS. Authenticom violated the CFAA by continuing to access the DMS anyway.

The Ninth Circuit's decision in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), *cert. denied sub nom. Power Ventures, Inc. v. Facebook, Inc.*, 138 S. Ct. 313 (2017), is instructive. There, a social networking site called Power.com used Facebook users' accounts (with the users' permission) to transmit promotional messages over Facebook's systems. After this activity began, Facebook sent a cease-and-desist letter to Power.com instructing it to stop accessing Facebook's systems. *Id.* at 1063. The Ninth Circuit held that, under the CFAA, while Power.com might have had "arguable permission" to access Facebook's systems based on Facebook users' actions, once Facebook itself instructed Power.com to cease and desist from its activities, it "no longer had authorization to access Facebook's computers." *Id.* at 1067. So too here: once CDK made clear to Authenticom that it opposed Authenticom's access to its systems, Authenticom was no

longer authorized to access the DMS, and its continued access violated the CFAA (and the parallel state laws).

Notably, the "agent" provision in the MSA makes no difference to this analysis. For the reasons we have explained above, that provision did not allow dealers to give DMS access to Authenticom. But even if it did, Authenticom's access to the DMS over CDK's express objection would still violate the CFAA and the parallel state laws. Dealers offended by CDK's efforts to block Authenticom could complain to CDK that CDK (in their view) was not honoring the terms of the MSA, but Authenticom cites no authority suggesting that a purported contractual obligation deprives a system owner of the ability to control access to its computer system for CFAA purposes. Thus, even if Authenticom were right about the meaning of the MSA (and it is not), Counts 1, 4, and 6 could not be dismissed.

Finally, Authenticom's observation that CDK's subsidiaries (DMI and IntegraLink) have provided integration services on other DMSs merits a brief response. CDK's subsidiaries formerly engaged in what CDK refers to as hostile integration on The Reynolds and Reynolds Company's DMS—but in 2015, in part out of recognition of the legal risks of this activity, CDK wound down DMI and IntegraLink's access to the Reynolds DMS and got out of the business of hostile integration altogether, as the earlier briefing in this case has described at length. In any event, the legality *vel non* of DMI and IntegraLink's hostile integration is not an issue here, either for purposes of this motion or the case generally. Because CDK has stated a claim that Authenticom accessed CDK's DMS without authorization, Authenticom's motion to dismiss CDK's CFAA claim must be denied.

B. CDK has stated a claim under the DMCA (Count 2)

Authenticom argues that it cannot be liable under the Digital Millennium Copyright Act ("DMCA") because it is immune from liability as an "authorized user of the CDK DMS" (Mot. 12); because CDK has not alleged "circumvent[ion]" of a technological measure under the DMCA (*id.* at

13); and because it falls within a statutory exception for conduct meant to "enable interoperability" of computer programs (*id.* at 15). It is wrong on all three counts.

First, Authenticom's claim to be exempt from liability as an authorized user is deficient for the reasons given above: CDK alleges that Authenticom is *not* authorized to access the DMS, and Authenticom's argument to the contrary cannot be resolved on a motion to dismiss. The holdings in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178, 1204 (Fed. Cir. 2004), and *Ticketmaster L.L.C. v. Prestige Entertainment, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018), are distinguishable on this point: *Chamberlain* turned on the fact that no right of the copyright holder was infringed by the alleged circumvention because the customers performing it were entitled under the Copyright Act to use the copy of the copyrighted software embedded in their garage door openers. 381 F.3d at 1204. And *Ticketmaster* simply stated in dicta that "legitimate users" of a website would not circumvent technological access measures by using them. 306 F. Supp. 3d at 1174. Authenticom, for the reasons given above, is not a "legitimate user" of the DMS.

Second, Authenticom's argument that it does not engage in unlawful "circumvention" under the DMCA is wrong. Authenticom first contends that use of dealer credentials, without authorization, is not "circumvention" under the DMCA. Mot. 13-14. But Authenticom did not simply use dealer-provided credentials without authorization; after CDK disabled login credentials that Authenticom had been using, Authenticom assisted dealers, including by automated means, to establish different credentials or to reinstate the disabled credentials. Counterclaim Compl. ¶¶ 63, 88-89, 108. *That* conduct circumvented CDK's technological measure of disabling credentials used by integrators, making it a moot point whether the unauthorized use of credentials, by itself, is unlawful circumvention.

Authenticom relatedly argues that it does not "circumvent" challenge prompts and CAPTCHAs by "responding" to them. Mot. 14. But that argument contradicts the plain language of the DMCA. A CAPTCHA is a "security measure" intended to "prevent and discourage the use of

automated programs" to access a system. *Ticketmaster*, 306 F. Supp. 3d at 1169; *see also* Counterclaim Compl. ¶ 92. CDK's challenge prompts are similarly designed to filter out human users from automated ones. Counterclaim Compl. ¶ 84. Authenticom, which uses automated means to access DMSs like CDK's, thus clearly "avoids" and "impairs" these measures by accessing CDK's system in the manner it admits it engages in. *See Ticketmaster*, 306 F. Supp. 3d at 1174 ("By using bots or CAPTCHA farms, Defendants are 'avoiding' CAPTCHA without the authority of Ticketmaster.").

Authenticom's argument that CDK cannot maintain a DMCA claim based on this circumvention because "nothing in its MSA . . . would restrict a dealer's ability either to employ automated access methods itself or to authorize agents to do so on its behalf" (Mot. 12 n.7) is a red herring. The reference to "agents" is simply a repackaged version of Authenticom's argument that the MSA permits dealers to give DMS access to whomever they want—which CDK has shown is both wrong and not grounds for dismissal in any event. And the notion that a hypothetical dealer (with an in-house software department) could employ automated access methods itself is speculative and irrelevant. Authenticom does not deny that security measures designed to catch automated access were an effective means of targeting access by hostile integrators, because hostile integrators generally use automated access methods and dealers generally do not. (If dealers could access the DMS directly by automated means and perform the necessary functions themselves, there would be little demand for data "integrators" like Authenticom in the first place.)

Lastly, Authenticom argues that its conduct was protected by the exception for reverse engineering—*i.e.*, efforts to make one computer program interoperable with another—in 17 U.S.C. § 1201(f)(2). Mot. 14-15. But that argument also fails. "[Section] 1201(f) is an affirmative defense" (*Chamberlain*, 381 F.3d at 1200 n.15), and an affirmative defense can only be a basis for dismissal if "the allegations of the complaint itself set forth everything necessary to satisfy the affirmative defense" (*United States v. Lewis*, 411 F.3d 838, 842 (7th Cir. 2005)). CDK's counterclaim complaint

does not come close to pleading the elements of Authenticom's purported reverse-engineering defense, and the defense would not defeat CDK's claim in any event, for two reasons.

First, Authenticom does more than simply provide "interoperability" between CDK's DMS and other software programs; it also extracts data from the DMS and copies it to its own system (Counterclaim Compl. ¶ 41) and creates copies of portions of the DMS program code, along with many of the DMS's unique and valuable features (*id.* ¶ 45), among other things. These activities are not privileged or protected under Section 1201(f)(2). *See, e.g.*, *Gen. Motors L.L.C. v. Autel. US Inc.*, 2016 WL 1223357, at *8 (E.D. Mich. Mar. 29, 2016) (denying motion to dismiss based on Section 1201(f)(2) where defendant allegedly made improper copies of plaintiff's proprietary software).

Second, Authenticom claims only the benefit of Section 1201(f)(2), not Section 1201(f)(1). Mot. 15. And Section 1201(f)(2), by its terms, is only a defense to Section 1201(a)(2) and 1201(b)'s anti-trafficking provisions, not to Section 1201(a)(1)'s prohibition on unauthorized circumvention of technological measures. *See* 17 U.S.C. § 1201(f)(2) ("Notwithstanding the provisions of subsections (a)(2) and (b) . . ."). Thus, even if the Court both accepted Authenticom's "interoperability" defense *and* were inclined to decide the issue on a motion to dismiss, CDK's claim of unlawful circumvention under Section 1201(a)(1)(A) could not be dismissed.

C. CDK has stated claims for misappropriation of trade secrets (Counts 3 and 5)

Authenticom argues that CDK has not stated a claim for misappropriation of trade secrets under the Defend Trade Secrets Act or the Wisconsin Uniform Trade Secrets Act because CDK has not "identifie[d] with any particularity which aspects of the DMS it alleges are trade secrets."[5] Mot. 15. But Authenticom is mistaken. CDK is "not required to compromise its trade secrets" by alleging them with painstaking specificity. *Chatterplug, Inc. v. Digital Intent, LLC*, 2016 WL 6395409, at *3 (N.D. Ill. Oct. 28, 2016). Indeed, "[c]ourts are in general agreement that trade secrets need not be

[5] Authenticom's other argument on these claims is a rehash of its authorization argument (Mot. 15-16), which fails for the reasons stated above.

disclosed in detail in a complaint alleging misappropriation for the simple reason that such a requirement would result in public disclosure of the purported trade secrets." *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 920–21 (N.D. Ill. 2001) (quoting *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 755 F. Supp. 635, 636 (D. Del.1991)). Thus, it is sufficient for pleading purposes if a complaint identifies the trade secrets at issue with sufficient specificity to provide "notice as to the substance of the claims." *Id.* at 921; *see also Chatterplug*, 2016 WL 6395409, at *3 (question is whether defendants can "discern what trade secrets are at issue"). CDK's complaint identifies the protected aspects of the DMS with ample specificity for those purposes, alleging that the DMS contains (1) forms used by dealers, (2) accounting rules, (3) tax tables, (4) proprietary tools, such as programs used to make calculations for financing transactions,[6] and (5) data compilations amassed from the data on the DMS. Counterclaim Compl. ¶¶ 48, 115.[7] Authenticom's motion to dismiss should therefore be denied as to these claims. And at a minimum, if the Court held that these allegations were not specific enough, the proper remedy would be dismissal without prejudice to replead. *See, e.g., Chatterplug*, 2016 WL 6395409, at *3.

D. CDK has stated a claim for trespass to chattels (Count 9)

Here again, Authenticom's only defense to CDK's trespass-to-chattels argument is that the MSA authorized it to access CDK's DMS. Mot. 17. As we have shown, that argument is wrong and, in any event, cannot be resolved in Authenticom's favor on a motion to dismiss. And for the reasons

[6] Authenticom argues that this cannot be a trade secret because it amounts to nothing more than a "basic math calculation—readily available on the Internet." Mot. 17. But the counterclaim does not allege that a calculation itself is a trade secret; rather, it alleges that dealers make such calculations using CDK's proprietary programs and data sets. Counterclaim Compl. ¶ 48. The latter are *not* "readily available" on the Internet or anywhere else.

[7] Contrary to Authenticom's implications, CDK's allegations are far more specific than the ones rejected in *Thermal Zone Products Corp. v. Echo Engineering, Ltd.*, 1993 WL 358148, at *1 (N.D. Ill. Sept. 14, 1993), and *Chatterplug*. The complaint in *Thermal Zone* offered nothing more than "blanket generalizations." 1993 WL 358148, at *5; *see also AutoMed*, 160 F. Supp. 2d at 921 n.3 (describing *Thermal Zone* as an "extreme case[]" in which the complaint "merely recited statutory language"). And the operative complaint in *Chatterplug* relied on proprietary names for technologies unknown to the court or the defendants, which made it impossible for them to discern the "general contours of the alleged trade secrets that [plaintiff] is seeking to protect." 2016 WL 6395409, at *3. The counterclaim complaint here exhibits neither defect.

given in Part II.A above, even if Authenticom were right about the meaning of the MSA, the contract would not be a defense to CDK's trespass-to-chattels claim. CDK alleges that, from at least June 2015 on, CDK denied consent to Authenticom to access the DMS. Thus, even if that denial violated a separate contractual agreement with dealers (and it did not), CDK has clearly alleged that Authenticom's DMS access was not "consensual." Count 9 should not be dismissed.

E. CDK has stated a claim for conversion (Count 10)

Authenticom next argues that CDK has not stated a claim for conversion because it has not alleged that Authenticom "converted the entire DMS." Mot. 19.[8] But whether the defendant converted the "entire[ty]" of the plaintiff's property is not the correct standard, as Authenticom's own authorities reflect. Rather, the question is whether the defendant exercised such control over the plaintiff's property as to cause "serious interference with the rights of the owner to possess the property." *Bruner v. Heritage Cos.*, 593 N.W.2d 814, 818 (Wis. Ct. App. 1999). CDK's allegations easily satisfy this standard, because CDK alleges that Authenticom accesses and controls the servers that make up the DMS by using them to run its own data search queries, which seriously interferes with CDK's possessory rights by burdening the DMS and reducing its efficiency. *E.g.*, Counterclaim Compl. ¶¶ 51-55, 164-66. Other courts have held that similar allegations stated a claim. *See, e.g.*, *McLeodUSA Telecomms. Servs., Inc. v. Qwest Corp.*, 469 F. Supp. 2d 677, 700 (N.D. Iowa 2007) (counterclaim plaintiff stated a claim for conversion by alleging that counterclaim defendant used plaintiff's network to route calls without authorization). The result should be no different here.

F. CDK has stated a claim for unjust enrichment under Wisconsin law (Count 11)

Authenticom seeks to avoid CDK's unjust enrichment claim by pleading ignorance about which state's law is the basis for the claim.[9] But there is no mystery on this point: CDK's claim

[8] Authenticom's other argument regarding this claim is a rehash of its authorization argument (Mot. 18 ("Authorization is incompatible with conversion.")), which fails for the reasons stated above.

[9] Authenticom's substantive argument on the unjust enrichment claim repeats its authorization argument (Mot. 20-21), which fails for the reasons stated above.

arises under the common law of Wisconsin, where Authenticom conducted its business. *Cf.* Mot. 17-18 (citing Wisconsin case law in response to Counts 9 and 10). This Court can evaluate the claim notwithstanding any lack of specificity in CDK's counterclaim complaint. *See, e.g.*, *Boles v. Merscorp, Inc.*, 2008 WL 3971557, at *1 (C.D. Cal. Aug. 26, 2008) (concluding that "[a]lthough Plaintiff does not specify, [his quiet title] claim appears to arise under California state law" and evaluating it under that law); *Kuligowska v. GNC Franchising, Inc.*, 2002 WL 32131024, at *8 (W.D. Pa. Nov. 25, 2002) (accepting plaintiffs' averment in their opposition to motion to dismiss that claim arose under law of Arizona).[10] And under Wisconsin law, CDK has easily stated a claim of unjust enrichment.[11] The complaint alleges (Counterclaim Compl. ¶¶ 35, 40-42, 79, 168-72) each of the elements of unjust enrichment under Wisconsin law: "(1) a benefit conferred on the defendant by the plaintiff, (2) appreciation or knowledge by the defendant of the benefit, and (3) acceptance or retention of the benefit by the defendant under circumstances making it inequitable for the defendant to retain the benefit." *Watts v. Watts*, 405 N.W.2d 303, 313 (Wis. 1987).

G. CDK has stated a claim for fraud (Count 12)

Finally, Authenticom's arguments as to why CDK has purportedly failed to state a claim for common-law fraud are merely dressed-up versions of its core argument that it was authorized by the MSA to access CDK's DMS. That argument, as we have shown, is both wrong and inappropriate for resolution on a motion to dismiss. And in any event, even if the MSA permitted access by Authenticom as dealers' "agent" (which it did not), CDK's fraud claim could not be dismissed.

The elements of fraud are "(1) the defendant made a misrepresentation of fact; (2) the representation was untrue; (3) the defendant knew the representation was untrue or made it

[10] If the Court were inclined to dismiss CDK's unjust enrichment claim on this basis, the appropriate remedy would be a dismissal without prejudice to allow CDK to replead it under Wisconsin law. *See, e.g.*, *Avenarius v. Eaton Corp.*, 898 F. Supp. 2d 729, 740 (D. Del. 2012) (dismissing with leave to amend); *Everett Labs., Inc. v. River's Edge Pharm., LLC*, 2010 WL 1424017, at *6 (D.N.J. Apr. 8, 2010).

[11] Because unjust enrichment is a cause of action in Wisconsin, it is irrelevant whether it is a cause of action under other states' laws (Mot. 19-20).

recklessly; (4) the representation was made with intent to deceive and induce the plaintiff to act upon it to the plaintiff's pecuniary damage; and (5) the plaintiff believed the representation to be true and relied on it." *Tietsworth v. Harley-Davidson, Inc.*, 677 N.W.2d 233, 252 n.38 (Wis. 2004). CDK's complaint properly alleges each of these elements: (1) Authenticom represented that it was a dealer employee when accessing CDK's DMS; (2) that representation was false; (3) Authenticom knew it to be false; (4) Authenticom made the misrepresentation to induce CDK's system to permit it to access the DMS; and (5) CDK relied on the misrepresentations in permitting Authenticom to access the DMS, which caused CDK harm in several ways. Counterclaim Compl. ¶¶ 83-86, 92, 174-77.

Authenticom does not deny the adequacy of these allegations as a matter of pleading. It argues, instead, that its purported authorization to access the DMS trumps any claim of fraud. It claims that because it was an authorized "agent" of dealers, even if not an "employee," any falsity in its representations about being an "employee" was not material. Mot. 22. And it argues that because CDK (in Authenticom's view) had no contractual right to block Authenticom's access, CDK was not "justified in relying on Authenticom's responses . . . to impede Authenticom's access." *Id.*

However the Court interprets the MSA, these arguments still are unavailing. A misrepresentation is material as long as "the maker knows or has reason to know that the recipient regards it as important." *Radford v. J.J.B. Enters., Ltd.*, 472 N.W.2d 790, 794 (Wis. Ct. App. 1991) (citing Restatement (Second) of Torts § 538 (1977)). CDK's complaint alleges that Authenticom has known since at least June 2015—*before* CDK implemented any of the security measures that Authenticom defeated through fraud—that CDK considered Authenticom's access to the DMS to be unauthorized. Counterclaim Compl. ¶ 82. Thus, by the time Authenticom confronted those security measures, it knew or had reason to know that CDK considered the issue of whether a user was an authorized dealership "employee" to be material to whether that user would be permitted to access the DMS. It follows that Authenticom's representations to CDK were material, regardless of whose interpretation of the MSA is correct.

Authenticom's argument that CDK was not "justified" in relying on Authenticom's misrepresentations is equally flawed. Once again, whether or not the MSA permitted Authenticom's DMS access (and it did not) has nothing to do with whether CDK's reliance on the misrepresentations was justified.[12] The requirement of justifiable reliance does not turn on one or the other party's purported contractual rights; it is a requirement aimed at winnowing out fraud claims where the truth was (or should have been) obvious to the recipient of the misrepresentation. *See, e.g.*, *Hennig v. Ahearn*, 601 N.W.2d 14, 24 (Wis. Ct. App. 1999) ("The general rule in Wisconsin, as elsewhere, is that the recipient of a fraudulent misrepresentation is justified in relying on it, unless the falsity is actually known or is obvious to ordinary observation."). Here, the complaint alleges numerous facts demonstrating why it is *not* obvious to CDK when Authenticom, rather than a dealership employee, accesses the DMS. CDK put in place specific security measures—including an express textual prompt asking whether a user is a dealership "employee"— intended to ensure that a user really was a human dealership employee. Counterclaim Compl. ¶¶ 84, 90. Authenticom has responded to these prompts with specific misrepresentations falsely certifying that it is a human dealership employee. *Id.* ¶¶ 85, 92. Authenticom does not and cannot argue that it is not justifiable for CDK to rely on those specific misrepresentations. CDK has therefore stated a claim of fraud.

CONCLUSION

The motion to dismiss should be denied.

[12] Authenticom's only authority for this dubious argument, *Rubloff Development Group, Inc. v. SuperValu, Inc.*, 863 F. Supp. 2d 732, 748 (N.D. Ill. 2012), is readily distinguishable. There, the plaintiff developer alleged that the defendants, including a grocery store chain, had attempted to block the plaintiff's development project and that defendants had used misrepresentations to conceal that the grocery store chain was behind the opposition. The court held that it was "speculative" whether the misstatements caused the plaintiff's injuries, because there was little support for the notion that the plaintiff would have done anything differently, or defeated opposition to the project more quickly, had it known the truth. *Id.* The case had nothing to do with whether and when reliance on a misrepresentation is "justified." And there is no problem of causation here. CDK unambiguously alleges that if it always knew when Authenticom was attempting to access its systems without authorization, it would prevent Authenticom from doing so. Counterclaim Compl. ¶ 176. That is more than sufficient to allege that Authenticom's misstatements caused CDK's injury.

Dated: August 20, 2018

Respectfully submitted,

/s/ *Britt M. Miller*
Britt M. Miller
Michael A. Scodro
Matthew D. Provance
MAYER BROWN LLP
71 South Wacker Drive
Chicago, IL 60606
(312) 782-0600
bmiller@mayerbrown.com
mprovance@mayerbrown.com

Mark W. Ryan
MAYER BROWN LLP
1999 K Street NW
Washington, DC 20006
(202) 263-3000
mryan@mayerbrown.com

Counsel for Defendant
CDK Global, LLC

CERTIFICATE OF SERVICE

I, Britt M. Miller, an attorney, hereby certify that on August 20, 2018, I caused a true and correct copy of the foregoing **DEFENDANT CDK GLOBAL, LLC'S OPPOSITION TO PLAINTIFF'S MOTION TO DISMISS COUNTERCLAIMS**, to be filed **UNDER SEAL** and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the court's CM/ECF System.

/s/ Britt M. Miller

Britt M. Miller
MAYER BROWN LLP
71 South Wacker Drive
Chicago, IL 60606
Phone: (312) 782-0600
Fax: (312) 701-7711
E-mail: bmiller@mayerbrown.com